What is claimed is:

1. A method for authenticating an electronic message containing message data and an electronic address, comprising the steps of:

receiving the electronic message from a sender;

creating a digest of the message data;

appending a temporal stamp to the digest;

signing the digest and temporal stamp with a digital signature;

sending the digest, temporal stamp, and the digital signature to the electronic address; and

authenticating the digest, the temporal stamp, and the digital signature.

2. The method of claim 1, wherein the step of creating a digest comprises generating a one-way hash value from the electronic message.

3. The method of claim 1, wherein the step of creating a temporal stamp comprises using the time and the date which indicate when the electronic message was received.

4. The method of claim 1, wherein the step of sending the digest, the temporal stamp, and the digital signature comprises sending the electronic

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

message.

5. The method of claim 1, wherein electronic address is the electronic address of the sender.

6. The method of claim 4 wherein the step of sending the electronic message comprises attaching at least one legal protection of an official entity.

7. The method of claim 1 further comprising the step of:

storing a copy of the digest, the temporal stamp, and the digital signature in a log file.

8. The method of claim 7 further comprising the step of:

creating a digest of the log file;

appending a temporal stamp to the digest of the log file; and

signing the digest of the log file and temporal stamp with a digital signature.

9. The method of claim 1 wherein the step of authenticating further comprises the steps of:

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

verifying that the digital signature was signed by the official entity;

verifying the specific identity of the entity which signed the digital signature; and

authenticating the contents of the electronic message using the digest.

10. A method for authenticating an electronic message containing data and an electronic address of a recipient, comprising the steps of:

sending an electronic message from a sender to a sender client;

receiving the electronic message at the sender client;

creating, by the sender client, a hash value from the data;

sending the hash value and the recipient electronic address from the sender client to an authentication server;

generating an electronic postmark data structure by the authentication server, the electronic postmark data structure including the hash value and time and date information;

sending the electronic postmark data structure and the recipient electronic address from the authentication server to a recipient client; and

sending the electronic postmark data structure from the recipient client to a recipient at the recipient electronic address; and

authenticating the electronic postmark data structure at the recipient.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

11. The method of claim 10, wherein the step of generating an electronic postmark data structure includes generating a digital signature for inclusion in the electronic postmark data structure.

12. The method of claim 11, wherein the step of generating a digital signature includes generating a digital key.

13. The method of claim 12, wherein the step of authenticating the electronic postmark data structure includes using the digital key.

14. The method of claim 11, wherein the step of generating a digital key involves including the digital key with the digital signature.

15. The method of claim 10, wherein the step of sending the hash value includes using an authentication server which is an electronic postmark server.

16. A method for requesting authentication of an electronic message, performed by a sender client, comprising the steps of:

receiving message data and a recipient electronic address from a sender;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

creating a hash value from the message data;

establishing a connection with an authentication server; and

sending the hash value, the recipient electronic address, and an authentication request to the authentication server.

17. The method of claim 16, wherein the step of establishing a connection includes sender client and the authentication server using TCP/IP.

18. The method of claim 16, wherein the step of sending an authentication request includes requesting an electronic postmark data structure for the authentication.

19. The method of claim 18, wherein the step of establishing a connection with an authentication server includes using an electronic postmark server.

20. A method for receiving authentication of an electronic message, performed by a receiver client, comprising the steps of:

receiving a recipient electronic address and an electronic postmark data structure from an authentication server, the electronic postmark data structure including time and date information; and

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

sending the electronic postmark to a recipient at the recipient electronic address.

21. The method of claim 20, wherein the step of receiving the electronic message involves communicating between the receiver client and the authentication server using TCP/IP.

22. The method of claim 20, wherein the step of receiving the electronic message from an authentication server involves using the authentication server which is an electronic postmark server.

23. The method of claim 20, further comprising the step of:

verifying the electronic postmark data structure using a digital key.

24. The method of claim 23, wherein the step of verifying the electronic postmark data structure involves including the digital key with the electronic postmark data structure.

25. The method of claim 20, wherein the step of receiving a recipient electronic address and an electronic postmark data structure further includes the

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

step of receiving the electronic message.

26. The method of claim 20, wherein the step of sending the electronic postmark data structure to a recipient further includes the step of sending the electronic message.

27. A method for authenticating an electronic message, performed by an authentication server, comprising the steps of:

receiving a request to authenticate the electronic message, the request including a recipient electronic address and a hash value corresponding to the electronic message;

creating an electronic postmark data structure for the electronic message, the electronic postmark data structure including time and date information;

generating a digital signature for the electronic postmark data structure;

including the digital signature in the electronic postmark data structure;

generating a public digital key for a recipient;

exporting the public digital key to a key authenticator for authorizing; and

sending the electronic postmark data structure and the recipient electronic address to a recipient client for delivery to the recipient at the recipient electronic address.

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

28. The method of claim 27, further comprising the steps of:

obtaining a authorized digital key for the electronic postmark data structure from a key authenticator, wherein the recipient can use the authorized digital key to verify the electronic postmark data structure; and

sending the authorized digital key to the receiver client.

29. The method of claim 27, wherein the step of receiving a request further involves including the electronic message in the request.

30. The method of claim 27, wherein the step of sending the electronic postmark data structure to a recipient client includes sending the electronic message to the recipient client.

31. The method of claim 27, wherein the step of exporting the public digital key to a key authenticator involves using a one of a key signing authority and a certificate authority.

32. A method for authenticating an electronic message, comprising the steps of:

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

receiving (1) a request to authenticate the electronic message and (2) a hash value derived from the electronic message, at a transaction processor from a sender client;

sending the request and the hash value from the transaction processor to an electronic postmark module for postmark processing;

obtaining, by the electronic postmark module, time and date information from a time module;

obtaining, by the electronic postmark module, branding data from a system registry;

generating, by a cryptographic device via a cryptographic interface module, a digital signature for the electronic message;

generating a public digital key for a recipient by a cryptographic device via a cryptographic interface module;

exporting the public digital key to a key authenticator by a key manager graphical user interface for key authorizing;

creating an electronic postmark data structure by the electronic postmark module, the electronic postmark data structure comprising the hash value, the time and date information, the branding data, and the digital signature;

storing a record of the postmark processing by the electronic postmark module in a log module;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

transmitting the electronic postmark data structure from the electronic postmark module to the transaction processor; and

transmitting the electronic postmark data structure from the transaction processor to a recipient client.

33. The method of claim 32, further comprising the steps of:

obtaining a authorized digital key for the electronic postmark data structure from the key authenticator, wherein the recipient can use the authorized digital key to verify the electronic postmark; and

sending the digital key to the recipient client.

34. The method of claim 32, wherein the step of obtaining time and date information from a time module includes using at least one hardware clock.

35. The method of claim 32 wherein the step of exporting the public digital key to a key authenticator involves using a key authenticator which is one of a key signing authority or a certificate authority.

36. The method of claim 32, further comprising the step of:

receiving updates to the time and date information in the time module via

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

a time manager graphical user interface.

37. The method of claim 32, wherein the step of obtaining branding data from a system registry includes using a Windows NT® system registry.

38. The method of claim 32, further comprising the step of:

interfacing with the system registry via a configuration manager graphical user interface.

39. The method of claim 32, further comprising the step of:

interfacing with the cryptographic interface module via the key manager graphical user interface.

40. The method of claim 32, wherein the step of receiving a request to authenticate involves receiving the electronic message.

41. The method of claim 32, wherein the step of transmitting the electronic postmark data structure to a recipient client involves transmitting the electronic message.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

42. A method for authenticating an electronic message, comprising the steps of:

sending a message comprising message data and a recipient electronic address from a sender to a sender front-end module at a sender client;

transmitting the message from the sender front-end module to a sender client proxy module at the sender client;

creating, by the sender client proxy module, a hash value from the message data;

sending the hash value and the recipient electronic address from the sender client proxy module via a network client module to a network server module at an authentication server;

generating an electronic postmark for the hash value by the authentication server, the electronic postmark including time and date information;

sending the electronic postmark and the recipient electronic address from the authentication server via a network client module on a recipient client to a recipient client proxy module on a recipient client;

transmitting the electronic postmark and the recipient electronic address from the recipient client proxy module to a recipient front-end module at the recipient client; and

sending the electronic postmark from the recipient client to a recipient at

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER, L. L. P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

the recipient electronic address.

43. The method of claim 42, wherein the step of generating an electronic postmark involves using the time and the date which indicate when the electronic message was received by the authentication server.

44. The method of claim 42, wherein the step of sending the hash value and the recipient electronic address to an authentication server involves using the authentication server which is an electronic postmark server.

45. The method of claim 42, further comprising the step of:

verifying the electronic postmark using a authorized digital key.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000